CYSE 201S – Journal Entries

Journal 1

One area I'd like to focus on for my career is cybersecurity policy and planning. I believe having knowledge on how to manage cybersecurity plans and their strategies is key for any job or career that heavily focuses on technology and the online world. Also, cybersecurity instruction is another focus I will consider, so I can help better the future of the cybersecurity workforce with information that has been educationally successful compared to things that haven't been as successful. Lastly, I want to focus on system security management which I feel is very similar to cybersecurity policy and planning. The one noticeable difference is instead of creating and implementing the policies on how to do stuff, a person is awarded the opportunity to dive into the work portion of cybersecurity.

Journal 2

These four scientific principles are related to cybersecurity through several ways. First empiricism mainly emphasizes data driven analysis and forensics to help us better understand threats and improve our cyber defenses. Secondly, determinism relates to cybersecurity through how cybersecurity outcomes can be predicted and mitigated by recognizing patterns in certain attack methods or system vulnerabilities. Thirdly, parsimony relates to cybersecurity through encouraging using the simplest, most direct approach, which is often the best. Lastly, objectivity ensures decisions are based on factual unbiased data such as threat severity or risk assessments rather than basic assumptions most people would make.

Journal 3

Researchers can utilize the Data Breach Chronology provided by Privacy Rights Clearinghouse to analyze patterns and trends in data breaches across the United States. This extensive database which includes over 70,000 incidents spanning nearly two decades, offers detailed information on the nature of breaches, the types of data compromised, and the entities involved. By examining this data, researchers can identify common vulnerabilities, assess the effectiveness of existing security measures, and evaluate the impact of breaches on affected individuals and organizations. Additionally, the database's interactive visualizations and detailed analyses can support the development of more robust data protection policies and strategies for the future.

Journal 4

Maslow's Hierarchy of Needs relates to technology in the following ways. For physiological needs: Technology helps meet basic needs, such as accessing food delivery apps or using health apps to track sleep or fitness, ensuring physical well-being. For Safety needs: things like secure banking apps or encrypted communication platforms, are pieces of technology that ensure financial and emotional safety, giving peace of mind. For Love and belonging social media platforms and messaging apps like WhatsApp enable connections with family and friends, which help create a sense of community and belonging. For Esteem needs Platforms like LinkedIn, Instagram, and gaming communities provide recognition and feedback, boosting self-esteem and offering validation for accomplishments. For Self-actualization Technology supports personal growth through online learning platforms, creative outlets like digital art tools such as photoshop and tools that encourage individuals to realize their full potential.

Journal 5

I ranked money first because cybercrimes motivated by financial gain is one of the most common and clear-cut motives for cyber-attacks. Hackers often target vulnerabilities for personal gain, whether through stealing credit card information, engaging in fraud, or ransomware attacks.

I ranked recognition second because the need for recognition and fame can drive hackers, particularly those who may want their exploits to be publicly known. Motivation for recognition can range from personal fame to public acknowledgment within certain subcultures.

I ranked political third because political motives for hacking have become more common in recent years, particularly with the rise of hacktivism. As shown in the article on youthful hackers joining the hacktivism wave, many individuals engage in cyberattacks to advance political causes or protest specific issues. I ranked it slightly lower than "For Money" and "Recognition" because financial motives often lead to more widespread and visible cyberattacks.

I ranked revenge fourth because as a motive revenge is also quite prevalent against individuals who have wronged the hacker. The article about revenge highlights how personal vendettas can lead to harmful cybercrimes. Although emotional motives like revenge can drive malicious activity, it’s not as high up as financial motivations because revenge tends to be more personal and isolated.

I ranked entertainment fifth because the desire for fun can certainly play a role in hacking, particularly among those who view hacking as a challenge or a way to test their skills or just for fun. The article discusses a LinkedIn scraping incident which could have been driven by the hacker's desire for entertainment or simply to prove their technical skill. While this is a valid motive, it seems less impactful than financial or political drives.

I ranked boredom sixth because it is an interesting but not very logical motive. Hacking to relieve boredom or because someone has nothing better to do can explain some low-level or trivial cybercrimes. However, compared to other motives. The article on cyberbullying hints at vulnerable individuals engaging in harmful acts due to boredom but this motive feels somewhat weaker compared to more direct motivations like revenge or financial gain.

I ranked multiple reasons last because this motive is way too broad and ambiguous, which makes it harder to rank clearly. While it's true that many hackers may have a combination of motivation, grouping them under "multiple reasons" doesn't provide much clarity. The article talks about various hackers' motivations and acknowledges the complexities, but it doesn't give enough specificity to make it a stronger motive so I ranked it last.

Journal 6

Fake sites displaying slight but unavoidable variations from the originals are the most common indicator. The most frequent indicator is a slight variation in the domain name. Fake sites typically have extra words or employ alternative domain extensions such as www.bank-xyz.com rather than "www.bankxyz.com"). On the other hand, legitimate sites possess a fixed and locked domain name like https://www.amazon.com missing on imitation sites is also HTTPS encryption. For example, there is no padlock in the address bar, leaving visitors open to attacks. Legitimate sites always employ HTTPS and indicate a secure connection. Design and content quality also differ. Fakes have poor-quality design, misspellings, and broken brands. They also may contain generic contact info, like generic email addresses or no contact info at all. Genuine sites have business quality high grade designs and possess clear easy to access contact information, such as managing customer service numbers and emails. When it comes to login pages and forms, phishing sites ask for too much sensitive information such as complete social security numbers or credit card numbers, typically via insecure forms. Genuine sites use secure login and multi-factor authentication and never ask for sensitive information via email. Secondly, fraudulent websites charge prices that are excessively low and unreasonable offers or discounting for a limited time. Genuine websites give fair prices, truthful conditions and a transparent payment process. Lastly, fraudulent websites usually engulf the users in advertisements or pop ups that compel them to make malware downloads. Genuine websites put checks on advertisements and do not urge dangerous downloads. By this type of seeking- the characteristics encompassing URL, security design, contact information, and price – you are better shielded from exploration by imitation sites.

Journal 7

Meme Caption: Average group size trying to code for a cyber assignment

Explanation: This meme represents the amount of people required to code for an average cyber assignment. This image depicts the level of difficulty coding requires for a group of humans to complete the task because, unlike a computer that operates quickly using software, humans need to use their brain power for coding assignments.

Journal 8

The video "Hacker Rates 12 Hacking Scenes in Movies" highlights how movies make hacking look more real than it is, shaping public opinion in misleading ways. Most movie depictions have hackers typing like maniacs, circumventing advanced security systems in matter of seconds, and gaining easy access to sensitive data. This over-dramatized representation of hacking is far from reality. In practice, cybersecurity is a complicated and meticulous undertaking requiring thorough expertise, perseverance, and time. The sensationalism by the media can create the wrong impression of cybersecurity that it is an easy job or a quick fix, contrary to the complex and risky undertaking it actually is.

Journal 9

I received a score of 2 on the questionnaire, and I feel that the survey questions were solid and relatable to the goal of the results that the survey is trying to accomplish. I believe that there are different patterns of internet usage around the world due to the multi levels of access and usage of the internet. It would make a lot of sense that someone in the United States would use the internet much more frequently than say a person from a country like Cuba or North Korea where access is difficult to obtain or completely cut off.

Journal 10

This social cybersecurity article identifies the increasing significance of cybersecurity in shaping human behavior, cultural, and political results. This branch of national security entails comprehending and predicting cyber-mediated societal change, affecting beliefs by technology on a scale previously unimaginable. As opposed to conventional cybersecurity, which is aimed at the security of information systems, social cybersecurity is aimed at human behavior through psychological manipulation using sophisticated tools such as network analysis, machine learning, and cognitive hacking. The article demonstrates how state and nonstate actors such as Russia employ information warfare to undermine societal trust and shape national values, and thus it is necessary for the Department of Defense to evolve to counter this emerging strategic threat. It's certain that as technology advances, the need to know about social cybersecurity will only grow, a change in how we are considering national security.

Journal 11

In the video "What Does a Cybersecurity Analyst Do? Salaries, Skills & Job Outlook", the job of a cybersecurity analyst is not just technical but also closely intertwined with social behavior. The video describes how cybersecurity analysts protect organizations from cyber-attacks, and the video emphasizes the growing need for security awareness and proactive internet behavior. Among the social issues underlying the video is the necessity of trusting online interactions—cybersecurity experts aim to make it possible for organizations and individuals to interact online safely, fostering good practices such as being careful when divulging personal data. The video further highlights the role of cybersecurity experts in educating users, thus shaping social norms in privacy, secure surfing habits, and the threats of cyber-attacks such as phishing. By safeguarding virtual spaces, analysts create a feeling of security, allowing users to interact more boldly in an increasingly digitizing world, ultimately shaping societal norms of technology uptake.

Journal 12

The sample data breach notification from Glasswasherparts.com highlights both economic and psychological theories. Rational Choice Theory applies as the company weighed the costs of notifying customers too early versus cooperating with law enforcement first. Laissez-Faire Theory appears in the reactive nature of the company's response, reflecting minimal regulatory interference. Psychologically, Neutralization Theory is evident as the company shifts blame to a third-party vendor, deflecting responsibility. Reinforcement Sensitivity Theory explains varied customer reactions—some may act quickly out of fear, while others may be reassured by the company's response. Together, these theories help explain both the business strategy and consumer behavior following a cybersecurity breach.

Journal 13

The literature review on bug bounty policies highlights their effectiveness in identifying cybersecurity vulnerabilities through incentivized crowdsourcing, where ethical hackers are paid to uncover weaknesses. Economically, these programs are cost-effective, offering access to a wide pool of expertise at a fraction of the cost of full-time security teams. Studies suggest that companies using bug bounty programs experience fewer security breaches and more robust cybersecurity. However, challenges like "false positives" and the need for structured submission review processes are also noted. While the economic benefits are clear, the review could have explored the social implications, particularly concerns about privacy when external hackers access internal systems. Overall, bug bounty policies are valuable tools for improving cybersecurity, but their success depends on clear guidelines and trust between companies and hackers.

Journal 14

The author, Andriy Slynchuk, provides a list of eleven things internet users do that may be illegal. The list incorporates a set of actions that, knowingly or unknowingly, are likely to have dire legal implications. Based on the level of severity, I feel the five most noteworthy violations are:

- Collecting personal information on children without the consent of parents is a serious crime which violates the Children’s Online Privacy Protection Act (COPPA). This violation can be used for exploitation and can cause tremendous damage to children’s safety.

- Impersonation on the internet may result in identity theft, fraud, and defamation. The act of impersonation can cause emotional distress and financial loss to the victim.

- Posting other people’s passwords, addresses, or photographs without their consent is an invasion of privacy rights and could result in stalking, harassment, or identity theft.

- Bullying and Trolling: online harassment of others can lead to severe psychological consequences for the victims like depression, anxiety, or even suicidal thoughts. Not only is this ethically unacceptable, but it is also legally liable in most parts of the world.

- Streaming on Unofficial Sites: pirated streaming on unofficial websites is a violation of intellectual property rights and puts users at risk of cybersecurity threats, including malware and phishing. These activities are especially grave since they violate people’s privacy, security, and well-being, and can result in severe legal consequences. Internet users need to know about them and practice responsible internet usage so as not to cause injury to others or get themselves into legal difficulties.

Journal 15

This video really made me see how much the social sciences are involved in this field. I had previously assumed that it was just a matter of technology and coding, but the speaker explained how understanding human behavior, motivation, and communication is just as important. He explained how his background in criminology and psychology allowed him to place digital evidence into the context of actual behavior. His own career path was not a linear one—he started out in criminal justice and later combined that with technical education. It made me realize that digital forensics isn't just about breaking technical puzzles, but attempting to comprehend the people behind the action. That blurring of lines between tech and human understanding makes the work worth doing and useful.